# EUROPEAN PATENT OFFICE

## Patent Abstracts of Japan


PUBLICATION NUMBER : 2001111543
PUBLICATION DATE : 20-04-01

APPLICATION DATE : 07-10-99
APPLICATION NUMBER : 11287262



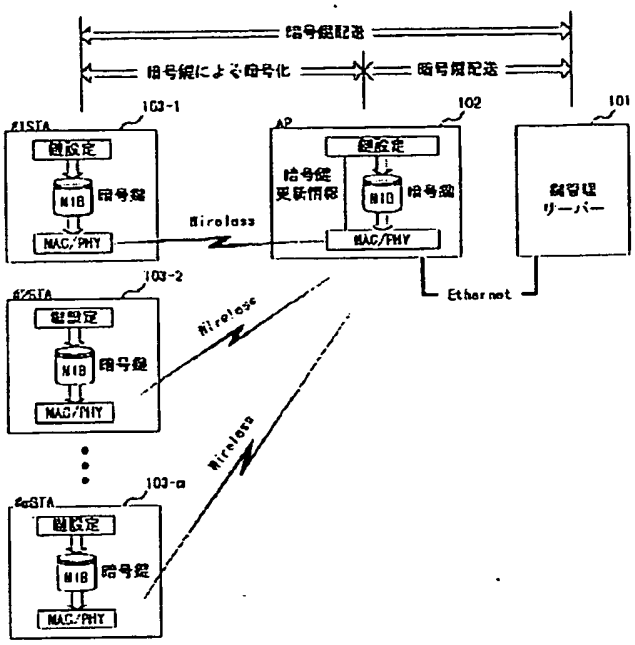
APPLICANT : NEC CORP;

INVENTOR : MORIMOTO SHINICHI;



INT.CL. : H04L 9/16 H04L 9/08 H04L 12/28


TITLE : CRYPTOGRAPHIC KEY UPDATE SYSTEM OF RADIO LAN AND UPDATING METHOD THEREFOR





ABSTRACT : PROBLEM TO BE SOLVED: To provide a cryptographic key update system and an updating method, capable of applying WEP of IEEE802.11 to a radio LAN system having many APs and STAs.

SOLUTION: This cryptographic key update system is constituted, so that a cryptographic key to be used for ciphering radio communication among all AP and STAs is defined as one set (k pieces), managed unitarily and distributed to each AP and STA, when the cryptographic key is updated by a key management server by providing the key management server connected with the AP by LAN.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－111543
(P2001－111543A)
(43)公開日　平成13年４月20日(2001.4.20)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード(参考) |
|---|---|---|---|---|
| Ｈ０４Ｌ　9/16 | | Ｈ０４Ｌ　9/00 | ６４３ | ５Ｊ１０４ |
| 9/08 | | | ６０１Ｅ | ５Ｋ０３３ |
| 12/28 | | | ６０１Ａ | |
| | | | ６０１Ｂ | |
| | | 11/00 | ３１０Ｂ | |

審査請求　有　請求項の数19　ＯＬ　（全 14 頁）

(21)出願番号　特願平11－287262

(22)出願日　平成11年10月７日(1999.10.7)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

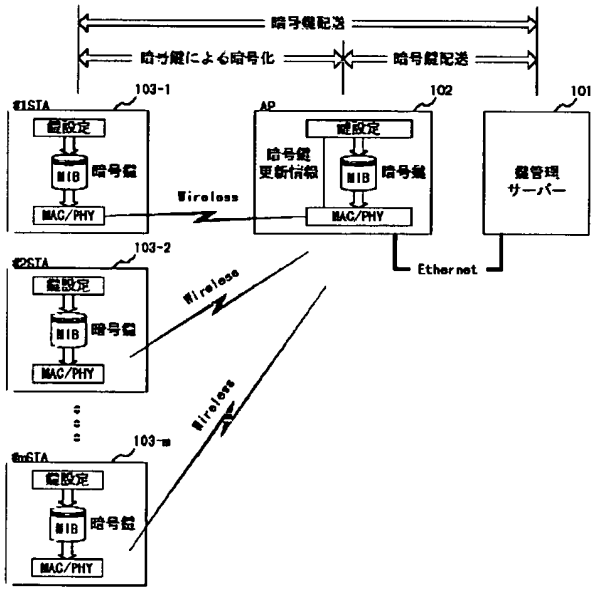
(72)発明者　森本　伸一
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　100082935
弁理士　京本　直樹　（外２名）

Ｆターム(参考)　5J104 AA01 AA16 AA34 EA01 EA18
MA05 NA02 NA37 PA00 PA07
5K033 AA08 BA13 CB01 CB03 CC04
DA01 DA17 DB10 DB12 DB14
EC01

(54)【発明の名称】　無線ＬＡＮの暗号鍵更新システム及びその更新方法

(57)【要約】
【課題】　複数のＡＰ、多数のＳＴＡを有する無線ＬＡＮシステムに、ＩＥＥＥ８０２．１１のＷＥＰを適用できる、暗号鍵更新方式及び更新方法を提供する。
【解決手段】　ＡＰとＬＡＮ接続された鍵管理サーバーを有し、全てのＡＰとＳＴＡの間の暗号化無線通信に使用する暗号鍵を１組（ｋ個）とし、一元管理するとともに、鍵管理サーバーにて暗号鍵を更新すると、各ＡＰ、及び各ＳＴＡに配送するよう構成している。



【特許請求の範囲】

【請求項１】ＬＡＮ上に１以上の無線アクセスポイント装置（ＡＰ）を有し、前記ＡＰは１以上の無線アクセス端末装置（ＳＴＡ）と無線接続し、前記ＳＴＡとの間でデータを暗号化して通信（暗号化通信）する無線ＬＡＮの暗号鍵更新システムにおいて、前記ＡＰとＬＡＮ接続された鍵管理サーバー装置（ＳＶ）は前記ＡＰと前記ＳＴＡの暗号化通信に使用するｋ個（ｋは１以上）の暗号鍵を記憶するＳＶ記憶手段と、前記暗号鍵を生成し前記ＳＶ記憶手段に格納する暗号鍵生成手段とを有し、前記ＳＶは、前記ＳＶ暗号鍵生成手段にて前記暗号鍵を生成して前記ＳＶ記憶手段に格納し、予め設定された条件に従って前記暗号鍵生成手段を制御して前記ＳＶ記憶手段に記憶した前記暗号鍵を更新し、更新した前記暗号鍵を前記ＡＰと前記ＳＴＡに配信する、ことを特徴とする、無線ＬＡＮの暗号鍵更新システム。

【請求項２】前記ＳＶは、前記ＳＶ記憶手段に記憶された前記暗号鍵を更新する時、前記暗号鍵生成手段にて１時に暗号鍵を１個生成し更新する、ことを特徴とする、請求項１に記載の無線ＬＡＮの暗号鍵更新システム。

【請求項３】前記ＳＶは、前記ＳＶ記憶手段に記憶された前記暗号鍵を更新する時、前記暗号鍵生成手段にて１時に前記暗号鍵を１個生成し、前記ＳＶ記憶手段に記憶されたｋ個の暗号鍵を所定間隔で１個ずつ順次に更新する、ことを特徴とする、請求項１に記載の無線ＬＡＮの暗号鍵更新システム。

【請求項４】前記ＳＶは、前記ＳＶ記憶手段に記憶されたｋ個の前記暗号鍵の内、（ｋ－１）個の暗号鍵については所定間隔（間隔１）で１個ずつ順次更新し、他の１個は（ｋ－１）個の暗号鍵より長い間隔（間隔２）で更新する、ことを特徴とする、請求項１に記載の無線ＬＡＮの暗号鍵更新システム。

【請求項５】前記ＡＰは、前記ＳＶの更新した第ｎ番（ｎは、１≦ｎ≦ｋ）の暗号鍵を配信されると前記ＡＰの記憶管理する第ｎ番の暗号鍵を更新する手段と、第ｎ番以外の暗号鍵を用いて暗号鍵更新通知伝文を暗号化して前記ＳＴＡに通知する手段とを有し、前記ＳＴＡは、前記ＡＰから前記暗号鍵更新通知伝文を受けるとＳＴＡ暗号鍵更新要求伝文を生成する手段と、前記暗号鍵更新通知伝文と同一の暗号鍵を用いて前記ＳＴＡ暗号鍵更新要求伝文を暗号化して前記ＡＰに通知する手段とを有し、前記ＡＰは、さらに、前記ＳＴＡから前記ＳＴＡ暗号鍵更新要求伝文を受けると前記ＳＶへＳＴＡ暗号鍵更新要求を通知する手段を有し、前記ＳＶは、さらに、前記ＡＰから前記ＳＴＡ暗号鍵更新要求を受けると前記ＳＴＡ宛て暗号鍵配送の可否を判断する手段と、可と判断した場合に前記ＡＰへ前記ＳＴＡ宛て暗号鍵を配送する手段とを有する、ことを特徴とする、請求項２乃至４の内、いずれか１に記載の無線ＬＡＮの暗号鍵更新システム。

【請求項６】前記ＡＰは、前記ＳＶの更新した第ｎ番（ｎは、１≦ｎ≦ｋ）の暗号鍵を配信されると前記ＡＰの記憶管理する第ｎ番の暗号鍵を更新する手段と、前記ＡＰの記憶管理するｋ個の暗号鍵の内、最初に更新された暗号鍵を用いて暗号鍵更新通知伝文を暗号化して前記ＳＴＡに通知する手段とを有し、前記ＳＴＡは、前記ＡＰから前記暗号鍵更新通知伝文を受けるとＳＴＡ暗号鍵更新要求伝文を生成する手段と、前記暗号鍵更新通知伝文と同一の暗号鍵を用いて前記ＳＴＡ暗号鍵更新要求伝文を暗号化して前記ＡＰに通知する手段とを有し、前記ＡＰは、さらに、前記ＳＴＡから前記ＳＴＡ暗号鍵更新要求伝文を受けると前記ＳＶへＳＴＡ暗号鍵更新要求を通知する手段を有し、前記ＳＶは、前記ＡＰから前記ＳＴＡ暗号鍵更新要求を受けると前記ＳＴＡ宛て暗号鍵配送の可否を判断する手段と、可と判断した場合に前記ＡＰへ前記ＳＴＡ宛て暗号鍵を配送する手段とを有する、ことを特徴とする、請求項２乃至４の内、いずれか１に記載の無線ＬＡＮの暗号鍵更新システム。

【請求項７】前記ＡＰは、さらに、前記ＳＶから前記ＳＴＡ宛て暗号鍵を配送されるとＳＴＡ暗号鍵配送伝文を生成する手段と、第ｎ番以外の暗号鍵を用いて前記ＳＴＡ暗号鍵配送伝文を暗号化して前記ＳＴＡに通知する手段とを有し、前記ＳＴＡは、さらに、前記ＡＰから前記ＳＴＡ暗号鍵配送伝文にて第ｎ番の暗号鍵を配送されると前記ＳＴＡの記憶管理する第ｎ番の暗号鍵を更新する手段を有する、ことを特徴とする、請求項５、または６に記載の無線ＬＡＮの暗号鍵更新システム。

【請求項８】前記ＡＰは、さらに、前記ＳＶから前記ＳＴＡ宛て暗号鍵を配送されるとＳＴＡ暗号鍵配送伝文を生成する手段と、ＡＰの記憶管理するｋ個の暗号鍵の内、最初に更新された暗号鍵を用いて前記ＳＴＡ暗号鍵配送伝文を暗号化して前記ＳＴＡに通知する手段とを有し、前記ＳＴＡは、さらに、前記ＡＰから前記ＳＴＡ暗号鍵配送伝文にて第ｎ番の暗号鍵を配送されると前記ＳＴＡの記憶管理する第ｎ番の暗号鍵を更新する手段を有する、ことを特徴とする、請求項５、または６に記載の無線ＬＡＮの暗号鍵更新システム。

【請求項９】前記ＳＴＡは、所定の要因を検出すると、ＳＴＡ暗号鍵一括更新要求伝文をＡＰへ通知する手段を有し、前記ＡＰは、前記ＳＴＡから前記ＳＴＡ暗号鍵一括更新要求伝文を受けると前記ＳＶへＳＴＡ暗号鍵一括更新要求を通知する手段を有し、前記ＳＶは、前記ＡＰから前記ＳＴＡ暗号鍵一括更新要求を受けると前記ＳＴＡ宛て暗号鍵一括配送の可否を判断する手段と、可と判断した場合に前記ＡＰへ前記ＳＴＡ宛て暗号鍵を一括配送する手段とを有し、前記ＡＰは、さらに、前記ＳＶから前記ＳＴＡ宛て暗号鍵の一括配送を受けるとＳＴＡ暗号鍵一括配送伝文を生成して前記ＳＴＡに通知する手段を有し、前記ＳＴＡは、さらに、前記ＡＰから前記ＳＴＡ暗号鍵一括配送伝文を受けると前記ＳＴＡの記憶する

暗号鍵を一括して更新する手段を有する、ことを特徴とする、請求項1乃至4の内、いずれか1に記載の無線ＬＡＮの暗号鍵更新システム。

【請求項１０】ＬＡＮ上に１以上の無線アクセスポイント装置（ＡＰ）を有し、前記ＡＰは１以上の無線アクセス端末装置（ＳＴＡ）と無線接続し、前記ＳＴＡとの間でデータを暗号化して通信（暗号化通信）する無線ＬＡＮの暗号鍵更新方法において、前記ＡＰとＬＡＮ接続された鍵管理サーバー装置（ＳＶ）は前記ＡＰと前記ＳＴＡの暗号化通信に使用するｋ個（ｋは１以上）の暗号鍵を生成するとともに記憶管理し、予め設定された条件に従って更新し、更新した前記暗号鍵を前記ＡＰと前記ＳＴＡに配信する、ことを特徴とする、無線ＬＡＮの暗号鍵更新方法。

【請求項１１】前記ＳＶは、前記ＳＶの記憶管理するｋ個の前記暗号鍵を更新する時、ｋ個の暗号鍵の内、１時に１個を更新する、ことを特徴とする、請求項１０に記載の無線ＬＡＮの暗号鍵更新方法。

【請求項１２】前記ＳＶは、前記ＳＶの記憶管理するｋ個の前記暗号鍵を更新する時、ｋ個の暗号鍵を所定間隔で１個ずつ順次に更新する、ことを特徴とする、請求項１０に記載の無線ＬＡＮの暗号鍵更新方法。

【請求項１３】前記ＳＶは、前記ＳＶの記憶管理するｋ個の前記暗号鍵の内、（ｋ－１）個の暗号鍵については所定間隔（間隔１）で１個ずつ順次に更新し、他の１個は（ｋ－１）個の暗号鍵より長い間隔（間隔２）で更新する、ことを特徴とする、請求項１０に記載の無線ＬＡＮの暗号鍵更新方法。

【請求項１４】前記ＡＰは、前記ＡＰの記憶管理する第ｎ番（ｎは、１≦ｎ≦ｋ）の暗号鍵を更新してから次に暗号鍵を更新するまでの間、前記ＡＰの記憶管理する第ｎ番以外の任意の暗号鍵を用いて前記ＳＴＡと暗号化通信する、ことを特徴とする、請求項１１乃至１３の内、いずれか1に記載の無線ＬＡＮの暗号鍵更新方法。

【請求項１５】前記ＡＰは、前記ＡＰの記憶管理する第ｎ番（ｎは、１≦ｎ≦ｋ）の暗号鍵を更新してから次に暗号鍵を更新するまでの間、前記ＡＰの記憶管理する第ｎ番以外の（ｋ－１）個の暗号鍵を順次用いて前記ＳＴＡと暗号化通信する、ことを特徴とする、請求項１１乃至１３の内、いずれか1に記載の無線ＬＡＮの暗号鍵更新方法。

【請求項１６】前記ＡＰは、前記ＡＰの記憶管理するｋ個の暗号鍵の内、最初に更新された暗号鍵を用いて前記ＳＴＡと暗号化通信する、ことを特徴とする、請求項１１乃至１３の内、いずれか1に記載の無線ＬＡＮの暗号鍵更新方法。

【請求項１７】前記ＳＴＡは、前記ＳＴＡの記憶管理する第ｎ番以外の（ｋ－１）個の暗号鍵の内、任意の暗号鍵を用いて前記ＡＰと暗号化通信する、ことを特徴とする、請求項１４乃至１６の内いずれか1に記載の無線ＬＡＮの暗号鍵更新方法。

【請求項１８】前記ＳＴＡは、前記ＳＴＡの記憶管理する第ｎ番以外の（ｋ－１）個の暗号鍵を順次用いて前記ＡＰと通信する、ことを特徴とする、請求項１４乃至１６の内いずれか1に記載の無線ＬＡＮの暗号鍵更新方法。

【請求項１９】前記ＳＴＡは、前記ＳＴＡの記憶管理するｋ個の暗号鍵の内、最後に更新された暗号鍵を用いて前記ＡＰと通信する、ことを特徴とする、請求項１４乃至１６の内いずれか1に記載の無線ＬＡＮの暗号鍵更新方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データを暗号化して無線通信する無線ＬＡＮシステムに関し、特にＷＥＰメカニズムによる暗号化を用いた無線ＬＡＮシステムにおける暗号鍵更新システム及びその更新方法に関する。

【０００２】

【従来の技術】従来、無線ＬＡＮシステムの普及に伴って、通信データの保護、すなわち、無線アクセスのセキュリティの確保が望まれていた。

【０００３】近年、屋外用途だけでなく、屋内向けにも無線ＬＡＮシステムの導入が進んでいる。例えば、構内にアクセスポイント（ＡＰ：固定の基地局）を設置し、フロア内に設置する端末装置に送受信装置（ＳＴＡ）を接続してＡＰとの間を無線化し、端末装置の配置変更の容易化、携帯型端末装置の帯出入に関する利便性向上を図るなどの例が増えている。

【０００４】このようなシステムにおいては、例えば外来者の持ちこむ携帯型無線端末装置や、屋外へ漏洩する電波を傍受可能な外部の無線端末装置に対して、通信データを保護する必要がある。

【０００５】無線通信におけるデータ保護の方式としては、暗号化を採用するものが一般化しつつある。無線データ通信における暗号化方式については、これまでＩＥＥＥで標準化の検討が進められてきた。

【０００６】現在のところ、無線区間の暗号化及び認証の方式としては、ＩＥＥＥ８０２．１１において、ＷＥＰ（The Wired Equivalent Privacy algorithm）メカニズムを使用した、Ｓｈａｒｅｄ Ｋｅｙ認証（共通鍵）方式が採用されている。

【０００７】図６（ａ）は、ＩＥＥＥ８０２．１１の８．２．３章に記載されている、ＷＥＰメカニズムによる暗号化方式を示すブロック図、（ｂ）は、同じく復号化方式を示すブロック図である。

【０００８】図６（ａ）に示すように、ＷＥＰメカニズムによる暗号化方式は、Ｓｅｅｄ生成手段６０１、暗号化手段６０２、誤り検出符号生成手段６０３、誤り検出符号付加手段６０４、及び暗号文生成演算手段６０５よ

り構成され、暗号化メッセージ606を出力する。暗号化手段602は、RC4アルゴリズムにより構成されている。

【0009】図6（a）の動作についてはIEEE802.11ドラフト中に記載があるので説明を省略するが、図6（a）の暗号化方式は、イニシャライゼーションベクタ（IV）、秘密鍵（Secret Key）、及び通信データ（Plaintext）を入力し、IVと暗号文（Ciphertext）を出力する。

【0010】図6（b）に示す、WEPメカニズムによる復号化方式は、Seed生成手段611、暗号化手段612、復号化演算手段613、符号分離手段614、誤り検出符号生成手段615、誤り検出符号比較手段616により構成されている。暗号化手段612は、RC4アルゴリズムにより構成されている。

【0011】図6（b）の復号化方式は、受信した暗号化メッセージ606からIVと暗号文を入力し、復号方式側で予め設定され、記憶している秘密鍵を使用して復号演算処理を行う。この結果、復号した平文（Plaintext）と、誤り検出符号（ICV）比較結果を出力する。

【0012】図7は、図6（a）から（b）へ伝送される暗号化メッセージ606の構成を示す。暗号化メッセージ606の構成は、拡張WEPフレームと称される。図7において各構成要素中に示す数字は、Octets（8ビット、以下「バイト」と記す）を単位としている。拡張WEPフレームは4バイトのIV701と、1バイト以上のデータ（PDU）702、4バイトのICV703により構成されている。拡張WEPフレームのデータ702、及びICV703は暗号化（Encrypt）され、IV701は暗号化されずに伝送される。

【0013】IV701は、暗号化に使用する暗号鍵の識別情報を含んでいる。すなわち、図示する様に、IV701は3バイトのイニシャライズベクター本体704に、6ビットのパッド705と、2ビットの鍵ID（Key ID）706とからなる1バイトの情報707を付加して構成されている。

【0014】この鍵ID706は2ビットの情報で構成されているので、4つまでの暗号鍵を識別することができる。従って、IEEE802.11の、WEPメカニズムを使用した暗号化方式においては、4つまでの暗号鍵を識別管理し、運用することができる。

【0015】ところで、従来この種の無線通信に用いられる暗号化復号化技術、あるいは暗号通信装置としては、様々なものが提案されている。

【0016】例えば、特開平11-196081号公報を参照すると、送信局と受信局とからなる暗号通信装置に適用できる暗号鍵の更新技術が開示されている。特開平11-196081号公報の発明によれば、暗号化によるデータ通信の手順は次のようである。

【0017】すなわち、まず、送信側にて予備鍵を生成する。次に送信側にて暗号鍵を用いて暗号化した伝文により、予備鍵を送信する。送受信双方で予備鍵を暗号鍵として更新し、以降これを用いて暗号化、復号化を行い、データを通信する。

【0018】この発明を実施するための構成の特徴としては、第1に予備鍵の記憶手段を有していること、第2に暗号鍵の記憶手段を有していること、第3に予備鍵を送信局が生成していることが挙げられる。

【0019】

【発明が解決しようとする課題】ところで、上記従来の暗号通信装置では、第1に鍵の管理を1対1で行っている。このため、そのままでは1対多のシステムへの応用が難しいという問題を有していた。

【0020】また、多くのSTAと、APとの間で無線アクセス環境を提供するシステムへの応用を考えた場合、APは、多くの端末のアクセスに使用する鍵を管理することとなる。例えばn台のSTAを有するシステムでは、APはn台分の暗号鍵を記憶管理する手段が必要となるので、回路規模が増大するとともに、処理の負荷が増大するという問題を有していた。

【0021】また、可搬型のSTAを使用者が持ち運んで移動したり、フロアのレイアウト変更などによってSTAが移設されることによって、それまでとは異なるAPにアクセスすることとなった場合には、STAとAPとで記憶管理している暗号鍵が不一致となり、通信できなくなるという問題を有していた。

【0022】さらに、特開平11-196081号公報の発明を1対多のシステムへ応用することを考えた場合、APは各STAに予備鍵を配送し、全てのSTAに予備鍵が行き渡った後、配布した予備鍵を暗号鍵として更新する手順が考えられる。しかしながら、このような手順で暗号鍵を更新しようとしても、全てのSTAが常時APにアクセスしているとは限らない状況においては、配送した予備鍵を暗号鍵に更新することができなくなる場合があるという問題を有していた。

【0023】従って、本発明の第1の目的は、多数のSTAと、APの間で行われる暗号化通信システムに適用可能な暗号通信装置を提供することにある。

【0024】また、多数のSTAがAPと通信する暗号化通信システムにおいて、容易に暗号鍵を生成、管理可能な暗号通信方式を提供することを第2の目的とする。

【0025】また、可搬型のSTAを移動したり、STAが移設されて、それまでとは異なるAPにアクセスすることとなった場合にも、新たなAPと、問題無くアクセスすることのできる暗号通信方式を提供することを第3の目的とする。

【0026】さらに、システムに属する全てのSTAがAPにアクセス可能な状態で無い場合にも随時暗号鍵を更新することで暗号化通信の信頼性を確保するととも

に、暗号鍵の更新されなかったＳＴＡに対する暗号鍵更新手順を設け、高い運用効率を有する暗号通信方式を提供することを第４の目的とする。

【００２７】

【課題を解決するための手段】上記の目的を達成するため、本発明の暗号鍵更新方式は、１以上のＡＰとＬＡＮ接続された鍵管理サーバーを有し、全てのＡＰとＳＴＡの間の暗号化無線通信に使用する暗号鍵を１組（ｋ個）とし、一元的に管理するとともに、各ＡＰ、及び各ＳＴＡに配送するよう構成している。

【００２８】本発明の暗号鍵更新方式のＡＰは、ｋ個の暗号鍵記憶手段を有し、鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照してＳＴＡと暗号化通信するよう構成している。

【００２９】本発明の暗号鍵更新方式のＳＴＡは、ｋ個の暗号鍵記憶手段を有し、ＡＰ経由で鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照してＡＰと暗号化通信するよう構成している。

【００３０】本発明の暗号鍵更新方式のＳＴＡは、暗号鍵記憶手段に記憶された全ての暗号鍵がＡＰと一致しない場合、ＡＰ経由で鍵管理サーバーに、暗号鍵の一括更新を要求し、鍵管理サーバーから暗号鍵を一括配送されるとＳＴＡにて記憶管理していた暗号鍵を更新し、これを参照してＡＰと暗号化通信するよう構成している。

【００３１】本発明の暗号鍵更新方法は、１以上のＡＰとＬＡＮ接続された鍵管理サーバーを有し、全てのＡＰとＳＴＡの間の暗号化無線通信に使用する暗号鍵を１組（ｋ個）とし、一元的に管理するとともに、各ＡＰ、及び各ＳＴＡに配送する。

【００３２】本発明の暗号鍵更新方法のＡＰは、ｋ個の暗号鍵記憶手段を有し、鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照してＳＴＡと暗号化通信する。

【００３３】本発明の暗号鍵更新方法のＳＴＡは、ｋ個の暗号鍵記憶手段を有し、ＡＰ経由で鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照してＡＰと暗号化通信する。

【００３４】本発明の暗号鍵更新方法のＳＴＡは、暗号鍵記憶手段に記憶された全ての暗号鍵がＡＰと一致しない場合、ＡＰ経由で鍵管理サーバーに、暗号鍵の一括更新を要求し、鍵管理サーバーから暗号鍵を一括配送されるとＳＴＡにて記憶管理していた暗号鍵を更新し、これを参照してＡＰと暗号化通信する。

【００３５】

【発明の実施の形態】以下に、本発明の実施の形態について、図面を参照して説明する。

【００３６】図１は本発明の実施の形態による無線ＬＡＮシステムの構成を示すブロック図である。図１に示す、本発明による無線ＬＡＮシステムは、鍵管理サーバー１０１、ＡＰ１０２、複数（ｍ台）のＡＰ（＃１ＳＴＡ１０３－１、＃２ＳＴＡ１０３－２、…＃ｍＳＴＡ１０３－ｍ）より構成されている。

【００３７】ＡＰ１０２とＳＴＡ１０３との間はＩＥＥＥ８０２．１１による無線（Ｗｉｒｅｌｅｓｓ）ＬＡＮ接続にて構成されている。

【００３８】ＳＴＡとＡＰとの間のデータ通信では、ＷＥＰメカニズムを使用した暗号化方式を用いる。ＷＥＰメカニズムを使用した暗号化方式では、ＳＴＡとＡＰは、それぞれ４個の暗号鍵を記憶管理し、暗号化、復号化を行う。

【００３９】図１の鍵管理サーバー１０１は、ＡＰ１０２とＳＴＡ１０３との間の無線区間において、暗号化に使用する暗号鍵を生成、管理する。鍵管理サーバーは新たな鍵を生成すると、ＡＰ１０２、ＳＴＡ１０３へ配送する。

【００４０】ＡＰ１０２は、鍵管理サーバー１０１から暗号鍵を配送されると、ＳＴＡ１０３との通信に使用する暗号鍵を更新し、記憶管理するとともに、ＳＴＡ１０３に暗号鍵の更新を通知する。

【００４１】ＳＴＡ１０３は、鍵管理サーバー１０１からＡＰ１０２を経由して配送された暗号鍵を記憶管理し、暗号鍵を使用してＡＰと通信する。

【００４２】図２は、ＡＰ１０２の構成を示すブロック図である。図２に示す、本発明によるＡＰ１０２は、制御手段２０１、暗号鍵設定手段２０２、第１鍵記憶手段２０３、第２鍵記憶手段２０４、第３鍵記憶手段２０５、第４鍵記憶手段２０６、鍵選択手段２０７、鍵ＩＤ生成手段２０８、ＩＶ生成手段２０９、平文入力手段２１０、ＷＥＰ暗号化手段２１１、暗号文送出手段２１２、暗号文入力手段２１３、ＷＥＰ復号手段２１４、平文出力手段２１５、及び、鍵ＩＤ抽出手段２１６より構成されている。

【００４３】ここで、ＷＥＰ暗号化手段２１１は、図６（ａ）にて説明した、ＩＥＥＥ８０２．１１のＷＥＰによる暗号化方式にて構成されている。また、ＷＥＰ復号化手段２１４は、図６（ｂ）にて説明したＩＥＥＥ８０２．１１のＷＥＰによる復号化方式にて構成される。

【００４４】図２に示す、第１乃至第４の鍵記憶手段２０３乃至２０６は、図１にも示すように、ＭＩＢと称されるバッファにより構成することができる。ＭＩＢはソフトウェアによって書換えることは可能であるが、ソフトウェアによって読み出すことは不可能な構造を持つ、情報秘匿性の高い記憶手段である。

【００４５】尚、図２に示す暗号鍵生成手段２００は、鍵管理サーバーに含まれる。

【００４６】図３は、ＳＴＡ１０３の構成を示すブロック図である。図３に示す、本発明によるＳＴＡ１０３は、制御手段３０１、暗号鍵設定手段３０２、第１鍵記憶手段３０３、第２鍵記憶手段３０４、第３鍵記憶手段３０５、第４鍵記憶手段３０６、鍵選択手段３０７、鍵

ＩＤ生成手段３０８、ＩＶ生成手段３０９、平文入力手段３１０、ＷＥＰ暗号化手段３１１、暗号文送出手段３１２、暗号文入力手段３１３、ＷＥＰ復号化手段３１４、平文出力手段３１５、及び、鍵ＩＤ抽出手段３１６より構成されている。図３に示す、第１乃至第４の鍵記憶手段３０３乃至３０６は、図２に示した鍵記憶手段と同様、ＭＩＢにより構成することができる。

【００４７】図４、図５は、本発明による無線ＬＡＮシステムにおける、暗号鍵の更新手順を示すシーケンスチャートである。

【００４８】図４は、通常の暗号鍵更新手順を示している。すなわち、ＳＴＡとＡＰは、互いに同じ暗号鍵を記憶管理している状態で、鍵管理サーバーが新たな暗号鍵を生成した場合に、ＡＰ、及びＳＴＡに配送し、更新する場合の手順である。

【００４９】図５は、ＳＴＡとＡＰとで記憶管理している暗号鍵が４個とも一致しない状態で、ＳＴＡの記憶管理する暗号鍵を更新する場合の手順を示す。すなわち、例えば、携帯型のＳＴＡ装置を長期に渡って帯出し、ＡＰ側の暗号鍵が全て更新された後に帯入してＡＰにアクセスしようとした場合、或いは、あるＳＴＡが長期に渡って稼動されることなく放置され、ＡＰ側の暗号鍵が全て更新された後に稼動された場合などに適用する、暗号鍵更新手順である。

【００５０】まず、通常の暗号鍵更新の動作について、図４、及び図１乃至図３を参照して説明する。

【００５１】図４において鍵管理サーバーは、４個の暗号鍵うち任意の１個（ｎ番）を新たに生成し、鍵管理サーバー内に記憶管理している第ｎ番目の暗号鍵を更新する（ｎ番の鍵更新）と、ＡＰに配送（ＡＰ鍵配送）する。

【００５２】ＡＰは鍵管理サーバーからＡＰ鍵配送を受けると、ＡＰ内に記憶管理している４個の内、第ｎ番目の暗号鍵を更新（ｎ番の鍵更新）し、ＳＴＡに対して鍵の更新を通知（鍵更新通知）する。この時、ＡＰからＳＴＡへ送信される鍵更新通知には、暗号鍵は含まれていない。ただ、ＡＰは第ｎ番以外の暗号鍵を用いて、鍵更新通知伝文を暗号化する。

【００５３】ここで、鍵管理サーバーからＡＰへ配送された暗号鍵の鍵ＩＤが１（ｎ＝１）であるとして、図２を参照して説明する。

【００５４】図２を参照すると、鍵管理サーバーの有する暗号鍵生成手段２００は、新たに暗号鍵を生成すると、ＡＰの制御手段２０１へ配送（ＡＰ鍵配送）する。ＡＰの制御手段２０１は、鍵管理サーバーから配送された暗号鍵と、鍵ＩＤ（１）を暗号鍵設定手段２０２へ転送する。暗号鍵設定手段２０２は、制御手段から受け取った暗号鍵を、鍵ＩＤに対応して第１鍵記憶手段２０３に格納し、更新する。

【００５５】次に制御手段２０１は、平文入力手段２１０と鍵ＩＤ生成手段２０８とを制御して、ＳＴＡへ鍵の更新を通知する。平文入力手段２１０は、制御手段からの制御により、鍵更新通知伝文を生成し、ＷＥＰ暗号化手段２１１に入力する。鍵ＩＤ生成手段２０８は、更新された鍵のＩＤとは違うＩＤを生成する。ここでは、例として鍵ＩＤ「２」を出力するものとする。鍵選択手段２０７は、第２鍵記憶手段２０４に記憶されている暗号鍵を選択し、ＷＥＰ暗号化手段２１１に入力する。ＩＶ生成手段２０９は、鍵ＩＤを２としたＩＶを生成し、ＷＥＰ暗号化手段２１１に入力する。

【００５６】ＷＥＰ暗号化手段２１１は、ＩＶ生成手段２０９から入力されたＩＶと、鍵選択手段２０７から入力された暗号鍵を使用して平文入力手段２１０から入力される鍵更新通知伝文を暗号化する。暗号文出力手段２１２は、ＷＥＰ暗号化手段２１１の作成した暗号文とＩＶを入力し、拡張ＷＥＰフレームを構成して送信装置などに出力する。

【００５７】図４に戻り、ＳＴＡは、ＡＰから鍵更新通知を受けると、ＡＰ経由で鍵管理サーバー宛てに鍵の更新を要求する。これを受けて、鍵サーバーはＳＴＡの真正性をチェックし、ＳＴＡ鍵配送可と判断すると、ＡＰ経由でＳＴＡ宛てに暗号鍵を配送する。ＳＴＡは、鍵管理サーバーからＳＴＡ鍵配送を受けると、新たな暗号鍵を記憶管理する。

【００５８】本発明による無線ＬＡＮシステムにおいては、ＳＴＡとＡＰ間の無線区間に以上の手順を採用することによって、より高い安全性を確保している。

【００５９】ＳＴＡが鍵更新通知を受け、鍵の更新を要求する動作について、図３を参照して説明する。

【００６０】図３を参照すると、ＡＰからの鍵更新通知は、暗号文入力手段３１３に入力され、ＩＶと暗号文に分けられて復号化手段３１４に入力される。ＷＥＰ復号化手段３１４は、入力されるＩＶを鍵ＩＤ抽出手段３１６へ出力する。鍵ＩＤ抽出手段３１６は、ＩＶ中の鍵ＩＤを取り出して鍵選択手段３０７を制御する。

【００６１】図２の動作説明でＩＶの鍵ＩＤは「２」としたので、鍵選択手段３０７は第２鍵記憶手段３０４を選択する。ＷＥＰ復号化手段３１４は、鍵選択手段３０７の出力する第２鍵を入力されて、鍵変更通知伝文を復号処理する。平文出力手段３１５は、ＷＥＰ復号化手段３１４の復号した平文を出力する。

【００６２】制御手段３０１は、平文出力手段３１５の出力を参照し、鍵更新通知を検出すると、鍵更新要求伝文を返送する。制御手段３０１は、鍵ＩＤ抽出手段３１６の出力する鍵ＩＤを参照し、鍵ＩＤ生成手段３０８へ転送する。鍵ＩＤ生成手段３０８は、制御手段から受け取った鍵ＩＤ「２」を出力する。鍵選択手段３０７はこれにより第２鍵記憶手段を選択する。ＩＶ生成手段３０９は、鍵ＩＤ「２」のＩＶを生成する。また、制御手段３０１は、平文入力手段３１０を制御して鍵更新要求伝

文を生成する。

【0063】WEP暗号化手段311は、IV生成手段309から入力されたIVと、鍵選択手段307から入力された暗号鍵を使用して平文入力手段310から入力される鍵更新要求伝文を暗号化する。暗号文出力手段312は、WEP暗号化手段311の作成した暗号文とIVを入力し、拡張WEPフレームを構成して送信装置などに出力する。

【0064】次に、STAから鍵更新要求を受けたAPが、鍵管理サーバーへ鍵更新要求伝文を送出し、鍵管理サーバーからのSTA鍵配送をSTAへ送出する動作について、図2を参照して説明する。

【0065】図2において、STAからの鍵更新要求伝文は、暗号文入力手段213に入力され、IVと暗号文に分けられて復号化手段214に入力される。WEP復号化手段214は、入力されるIVを鍵ID抽出手段216へ出力する。鍵ID抽出手段216は、IV中の鍵IDを取り出して鍵選択手段207を制御する。

【0066】STAの送出したIVの鍵IDは「2」であるので、鍵選択手段207は第2鍵記憶手段204を選択する。WEP復号手段214は、鍵選択手段207の出力する第2鍵を入力されて、鍵変更要求伝文を復号処理する。平文出力手段215は、WEP復号化手段214の復号した平文を出力する。

【0067】制御手段201は、平文出力手段215の出力を参照し、鍵更新要求を検出すると、鍵管理サーバーへ鍵更新要求伝文を送出する。

【0068】STAの出力する鍵更新要求伝文には、STA固有の情報を含み、鍵管理サーバーにて鍵配送の可否判断のため、参照される。すなわち、STAは、固有の情報として、STAのMACアドレス、STA使用者の識別情報、パスワードなどを鍵更新要求伝文に含めて送出する。

【0069】鍵管理サーバーはこれらSTAからの固有情報と、予め各STAに関して登録された固有情報とを比較する。そして、受け取った鍵更新要求伝文の送出元STAの真正性が確認された場合に限り、STA宛てに暗号鍵を配送する。

【0070】図2を参照すると、鍵管理サーバーの有する暗号鍵生成手段200は、STA宛ての暗号鍵をAPの制御手段201へ配送（STA鍵配送）する。APの制御手段201は、鍵管理サーバーから配送されたSTA鍵配送伝文を、平文入力手段210に入力する。次に鍵ID生成手段208を制御して、STAへ暗号鍵を配送する。平文入力手段210は、制御手段からのSTA鍵配送伝文を、WEP暗号化手段211に入力する。鍵ID生成手段208は、鍵ID「2」を出力する。鍵選択手段207は、第2鍵記憶手段204に記憶されている暗号鍵を選択し、WEP暗号化手段211に入力する。IV生成手段209は、鍵IDを2としたIVを生成し、WEP暗号化手段211に入力する。

【0071】WEP暗号化手段211は、IV生成手段209から入力されたIVと、鍵選択手段207から入力された暗号鍵を使用して平文入力手段210から入力されるSTA鍵配送伝文を暗号化する。暗号文出力手段212は、WEP暗号化手段211の作成した暗号文とIVを入力し、拡張WEPフレームを構成して送信装置などに出力する。

【0072】続いて、STAがSTA鍵配送伝文を受け、暗号鍵を更新する動作について、図3を参照して説明する。

【0073】図3を参照すると、APからのSTA鍵配送伝文は、暗号文入力手段313に入力され、IVと暗号文に分けられて復号化手段314に入力される。WEP復号化手段314は、入力されるIVを鍵ID抽出手段316へ出力する。鍵ID抽出手段316は、IV中の鍵IDを取り出して鍵選択手段307を制御する。

【0074】鍵選択手段307は鍵IDに従って、第2鍵記憶手段304を選択する。WEP復号化手段314は、鍵選択手段307の出力する第2鍵を入力されて、STA鍵配送伝文を復号処理する。平文出力手段315は、WEP復号化手段314の復号した平文を出力する。

【0075】制御手段301は、平文出力手段315の出力を参照し、STA鍵配送伝文を検出すると、受け取ったSTA鍵を暗号鍵設定手段302に転送する。暗号鍵設定手段302は、受け取った平文に含まれる、配送された暗号鍵のIDを参照して、対応する鍵記憶手段に格納し、暗号鍵を更新する。この例では、第1鍵を更新するので、平文には鍵ID「1」が含まれる。従って、新たな暗号鍵は第1鍵記憶手段303に格納される。

【0076】以上説明した動作によって、鍵管理サーバーの生成する暗号鍵をAP、及びSTA宛てに配送し、それぞれの記憶管理する暗号鍵を更新することができる。

【0077】次に、多数のSTA、及び、複数のAPに対する、暗号鍵の管理について説明する。

【0078】本発明の無線LANシステムでは、鍵管理サーバーに複数のAPが接続される場合がある。そして、システムに係属するSTAは、フロアレイアウトの変更、または、可搬型STAの移動によって、それまでとは別のAPにアクセスする場合も考えられる。これらの条件に鑑み、複数のAPに加え、多数のSTAの暗号鍵を容易に管理可能とするするため、本発明の無線LANシステムにおいては、鍵管理サーバーは、各AP、STAに配送する暗号鍵を、システム全体に渡って共通の1組（4個）としている。こうすることによって、管理する暗号鍵の数を最小限に留めてシステムの負荷を低減することができる。また、複数のAPに渡ってSTAを移動した場合にも、各APが同一の暗号鍵を有するの

で、暗号鍵不一致の発生を回避することができる。

【0079】次に、本発明の無線ＬＡＮシステムにおける、暗号鍵の更新、及びＳＴＡとＡＰにおける暗号鍵の運用について説明する。

【0080】ＩＥＥＥ８０２．１１のＷＥＰでは、４個の暗号鍵を識別して管理、運用することができる。そこで、本発明の無線ＬＡＮシステムでは、４個の暗号鍵の更新、及び、ＡＰとＳＴＡとがそれぞれ通信する場合の暗号鍵の運用について、次に示す幾つかの方法を採用し、高い運用性と情報秘匿性の両立を図っている。

【0081】暗号鍵更新方法の第１として、鍵管理サーバーは、４個の暗号鍵をある一定の期間が経過するごとに、１個ずつ順次更新していく。具体的には、１週間経過する毎に、１個ずつ順次更新する。こうすることによって、それぞれの暗号鍵は４週間に１度、更新されることとなる。従って、携帯型のＳＴＡを帯出する者は、４週間以内にＳＴＡを帯入すれば、問題無くＡＰにアクセスすることができる。

【0082】この期間の長さは、鍵管理サーバーにて設定可能としてもよく、システムの要求によって、例えば１日毎、１ヶ月毎などとしてもよい。

【0083】この要領で暗号鍵を更新するシステムでは、ＳＴＡとＡＰは次に示す、幾つかの方法で暗号鍵を運用する。

【0084】その１によれば、ＡＰは４個の暗号鍵の内、最後に更新した暗号鍵を通信に使用せず、他の３個を順次用いてＳＴＡと通信する。

【0085】複数のＳＴＡが存在するシステムにおいては、全てのＳＴＡの記憶管理する暗号鍵の更新には時間を要する。すなわち、暗号鍵の更新は鍵管理サーバーからＡＰ、ＳＴＡに対して個別に行われるため、ＡＰが暗号鍵を１個更新した時、各ＳＴＡはＡＰからの暗号鍵更新通知を受けて逐次鍵管理サーバーへ暗号鍵更新要求を行い、鍵管理サーバーから鍵配送を受けて個々に暗号鍵を更新する。

【0086】この方法を採用することによって、ＡＰが１個の暗号鍵を更新してから、全てのＳＴＡの記憶管理する暗号鍵の更新が完了するまでの間、暗号鍵の不一致に起因する障害を回避することが可能となる。

【0087】その２によれば、ＡＰは、最初に更新した暗号鍵を用いてＳＴＡと通信する。

【0088】こうすることによって、ＳＴＡはより長い期間に渡って暗号鍵更新の機会を得ることができる。

【0089】上記第１の暗号鍵の更新方法における、その１、及びその２の暗号鍵の使用方法において、ＳＴＡは、ＳＴＡの記憶管理する暗号鍵の内、最後に更新されたものを使用して通信する。こうすることによって、携帯型ＳＴＡの帯出可能期間、あるいはＳＴＡの非稼動可能期間を最も長くすることができる。尚、情報秘匿性向上のために、最後に更新された暗号鍵以外の暗号鍵を適宜利用してもよい。

【0090】暗号鍵更新方法の第２として、鍵管理サーバーは、特定の暗号鍵の更新周期を他の暗号鍵の更新周期よりも大幅に長く設定し、他の暗号鍵はより短い更新周期で順次更新する。具体的には、第１の暗号鍵は３ヶ月毎に更新し、第２乃至第４の鍵については、１日毎に１個ずつ順次更新する。こうすることによって、携帯型のＳＴＡを帯出する者は、３ヶ月以内にＳＴＡを帯入すれば、問題無くＡＰにアクセスすることができるので、利便性が向上するとともに、他の３個の暗号鍵は３日周期で更新されるため、これを通信に利用すれば情報秘匿性は向上する。

【0091】尚、この方法においても、暗号更新周期は、システムの要求によって、任意に定められてよいことは、云うまでも無い。

【0092】この要領で暗号鍵を更新するシステムでは、ＳＴＡとＡＰは次に示す、幾つかの方法で暗号鍵を使用することができる。

【0093】その１によれば、ＡＰは３日周期で更新される暗号鍵を適宜使用して、ＳＴＡと通信する。ＡＰと一致した暗号鍵を記憶管理しているＳＴＡも、３日周期で更新される暗号鍵を使用して通信することで、ＳＴＡとＡＰ間の通信における情報の秘匿性は高く保つことができる。しかしながら、ＳＴＡが３日以上帯出された後、帯入されてＡＰにアクセスする場合、あるいは、３日以上非稼動状態にあったＳＴＡが再度稼動されてＡＰにアクセスする場合には、暗号鍵の不一致を生じる。この場合ＡＰは、その２に示す方法により、ＳＴＡと通信する。

【0094】その２によれば、ＡＰはＳＴＡからの伝文の暗号鍵が、ＡＰにて記憶管理するものと不一致を生じた場合、３ヶ月周期で更新する暗号鍵を用いてＳＴＡとの通信を試みる。この方法で暗号鍵が一致した場合、ＡＰはＳＴＡに対して暗号鍵の更新を通知する。ＳＴＡはこれにより暗号鍵更新要求を行い、鍵管理サーバーから最新の暗号鍵を配送され、更新することができる。

【0095】ところで、上記第２の暗号鍵更新方法を用いても、３ヶ月を超えて長期に渡るＳＴＡの帯出、あるいは非稼動に対しては、全ての暗号鍵が不一致となる。

【0096】次に、このような場合の暗号鍵更新動作について、図５を参照して説明する。

【0097】図５を参照すると、ＡＰと一致する暗号鍵を有しないＳＴＡは、例えば第１鍵から順次ＳＴＡにて記憶管理している暗号鍵を使用して、ＡＰにアクセスを要求（アクセス要求１回目）する。ＡＰは、暗号鍵が一致しないので、平文を使用して鍵の不一致を通知（鍵ＮＧ通知１回目）する。

【0098】暗号鍵の不一致を４回繰り返すと、ＳＴＡは平文を利用して、鍵の一括更新を要求（鍵の一括更新要求）する。ＡＰは、ＳＴＡからの鍵の一括更新要求を

鍵管理サーバーへ転送する。このとき、暗号鍵の一括更新要求伝文には、ＳＴＡの個別情報が含まれることは、図４にて説明した動作と同様である。

【００９９】鍵管理サーバーはＳＴＡの個別情報をチェックし、真正性を確認すると、ＡＰ経由でＳＴＡ暗号鍵を一括して配送する。ＳＴＡは鍵管理サーバーからのＳＴＡ暗号鍵一括配送を受けると、記憶管理していた暗号鍵を一括して更新する。

【０１００】次にＳＴＡは、新たな暗号鍵を使用してＡＰにアクセスを要求する。ＡＰは暗号鍵を確認し、一致すると、通常のデータ通信を開始する。

【０１０１】尚、図５は、理解の容易のためＳＴＡは４回に渡ってアクセス要求するものとしているが、より効率的なシーケンスも考えられることは云うまでも無い。すなわち、ＳＴＡは４個の暗号鍵の内、最後に更新された暗号鍵を第１回目のアクセス要求に使用し、これが不一致となった場合には、直ちに鍵の一括更新を要求する、などのシーケンスが考えられる。

【０１０２】ところで、図５のシーケンスチャートにおいて、ＳＴＡの暗号鍵一括更新要求からＳＴＡ暗号鍵一括配送までの、ＳＴＡとＡＰ間の無線通信は、平文で行うものとしている。これは、図５は、ＡＰとＳＴＡの間の無線区間を含む、別途の暗号化通信を適用することを前提としているためである。

【０１０３】すなわち、図５上部に示すように、鍵管理サーバーからＳＴＡまでの区間において、あるいは、ＡＰからＳＴＡまでの区間において、公開鍵を使用するなどにより、本発明とは別途の暗号化復号化を併用することで、図５のシーケンスにおいて安全にＳＴＡの暗号鍵を更新することが可能となる。

【０１０４】本発明によれば、ＳＴＡの記憶管理する４個の暗号鍵の全てがＡＰと一致しない状態となっても、無線ＬＡＮシステムによって暗号鍵を一括更新する（すなわち、人間系によって暗号鍵をＳＴＡに設定するなどの作業を介さずに暗号鍵を更新可能とする）ことができる。

【０１０５】

【発明の効果】以上説明したように本発明によれば、１以上のＡＰとＬＡＮで接続された鍵管理サーバー装置を有し、全てのＡＰとＳＴＡの間の暗号化無線通信に使用する暗号鍵を１組（ｋ個）とし、鍵管理サーバー装置にて一元的に管理することによって、暗号鍵の管理のために装置の回路規模が増大することもなく、また、暗号鍵の管理のために処理の負荷が増大することもなく、容易に１対多の無線ＬＡＮシステムを提供することができる。

【０１０６】また、本は発明によれば、可搬型のＳＴＡを使用者が持ち運んで移動したり、フロアのレイアウト変更などによってＳＴＡが移設されることによって、それまでとは異なるＡＰにアクセスすることとなった場合にも、ＳＴＡと、ＳＴＡのアクセスするＡＰとの間で記憶管理している暗号鍵が不一致となることがない、無線ＬＡＮシステムを提供することができる。

【０１０７】さらに、本発明によれば、可搬型のＳＴＡを使用者が長期に帯出したためにＳＴＡの暗号鍵の更新がされず、再度帯入した時にはＳＴＡの記憶していた全ての暗号鍵が、アクセスしたＡＰと不一致する状態となった場合にも、ＳＴＡに対する暗号鍵の更新手順を提供するので、人間系の操作による煩雑な対応処置を必要とせずにＳＴＡの記憶していた暗号鍵を更新できる、高い運用性を有する暗号通信方式を提供することができる。

【図面の簡単な説明】

【図１】本発明の無線ＬＡＮシステムの構成を示すブロック図である。

【図２】本発明のＡＰの構成を示すブロック図である。

【図３】本発明のＳＴＡの構成を示すブロック図である。

【図４】本発明の暗号鍵更新手順を説明するためのシーケンスチャートである。

【図５】本発明の暗号鍵更新手順を説明するためのシーケンスチャートである。

【図６】従来の技術において、ＩＥＥＥ８０２．１１のＷＥＰによる暗号化方式を説明するためのブロック図である。

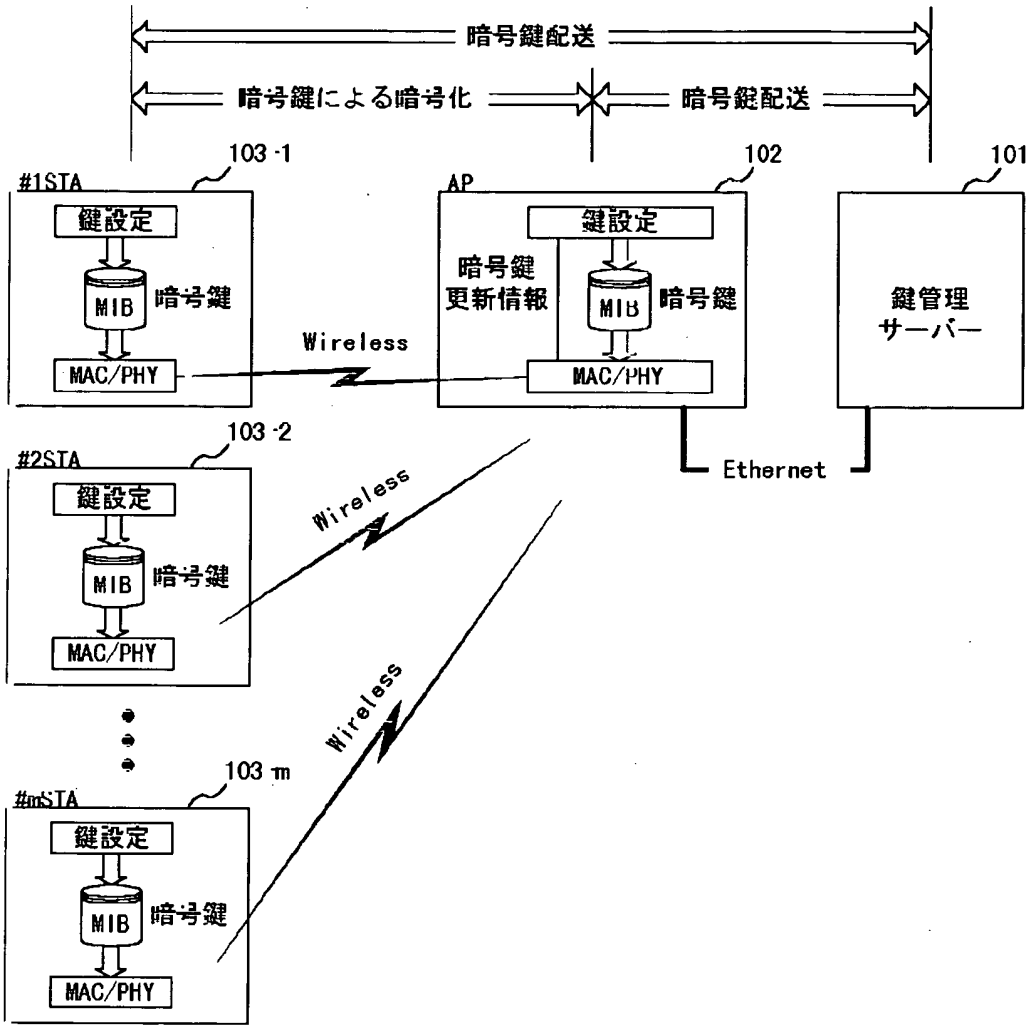
【図７】従来の技術において、ＩＥＥＥ８０２．１１のＷＥＰによる復号化方式を説明するためのブロック図である。

【符号の説明】

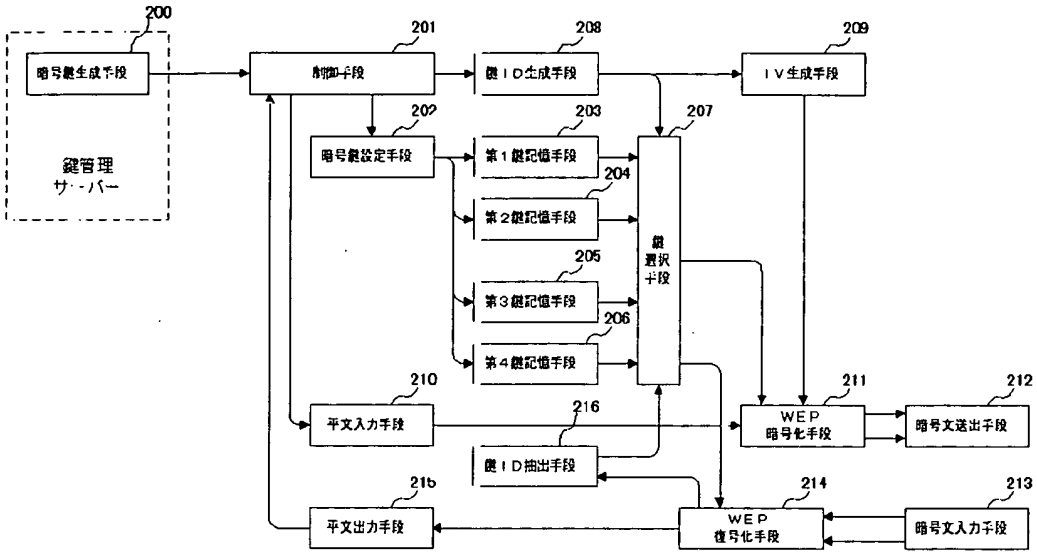
１０１　鍵管理サーバー
１０２　ＡＰ
１０３　ＳＴＡ
２００　暗号鍵生成手段
２０１　制御手段
２０２　暗号鍵設定手段
２０３　第１鍵記憶手段
２０４　第２鍵記憶手段
２０５　第３鍵記憶手段
２０６　第４鍵記憶手段
２０７　鍵選択手段
２０８　鍵ＩＤ生成手段
２０９　ＩＶ生成手段
２１０　平文入力手段
２１１　ＷＥＰ暗号化手段
２１２　暗号文送出手段
２１３　暗号文入力手段
２１４　ＷＥＰ復号化手段
２１５　平文出力手段
２１６　鍵ＩＤ抽出手段
３０１　制御手段
３０２　暗号鍵設定手段

303　第1鍵記憶手段
304　第2鍵記憶手段
305　第3鍵記憶手段
306　第4鍵記憶手段
307　鍵選択手段
308　鍵ID生成手段
309　IV生成手段
310　平文入力手段
311　WEP暗号化手段
312　暗号文送出手段
313　暗号文入力手段
314　WEP復号化手段
315　平文出力手段
316　鍵ID抽出手段

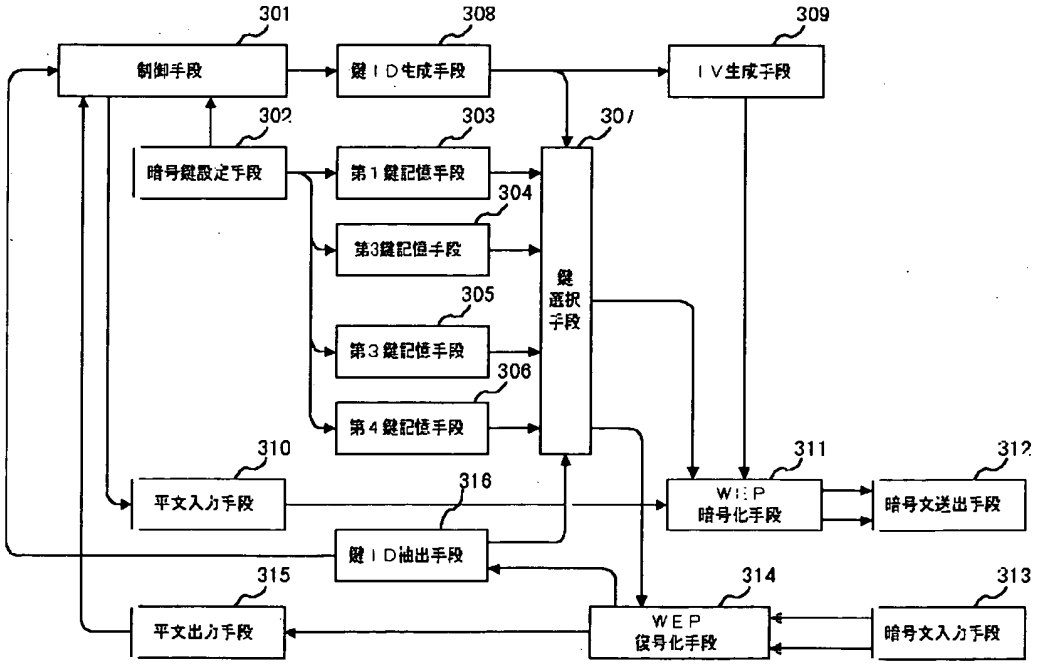
【図1】



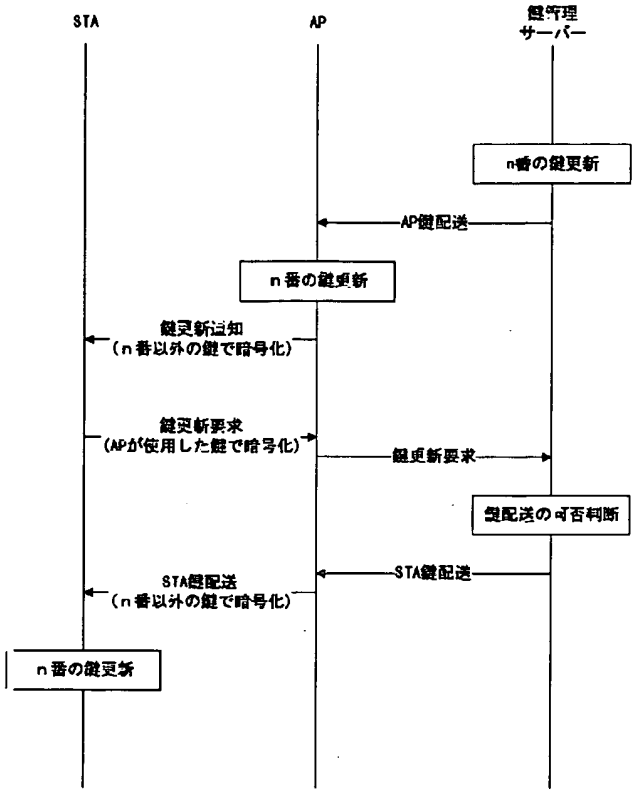
【図2】


200
暗号鍵生成手段
鍵管理
サーバー
201
制御手段
208
鍵ID生成手段
209
IV生成手段
202
暗号鍵設定手段
203
第1鍵記憶手段
204
第2鍵記憶手段
205
第3鍵記憶手段
206
第4鍵記憶手段
207
鍵選択手段
210
平文入力手段
216
鍵ID抽出手段
211
WEP暗号化手段
212
暗号文送出手段
215
平文出力手段
214
WEP復号化手段
213
暗号文入力手段

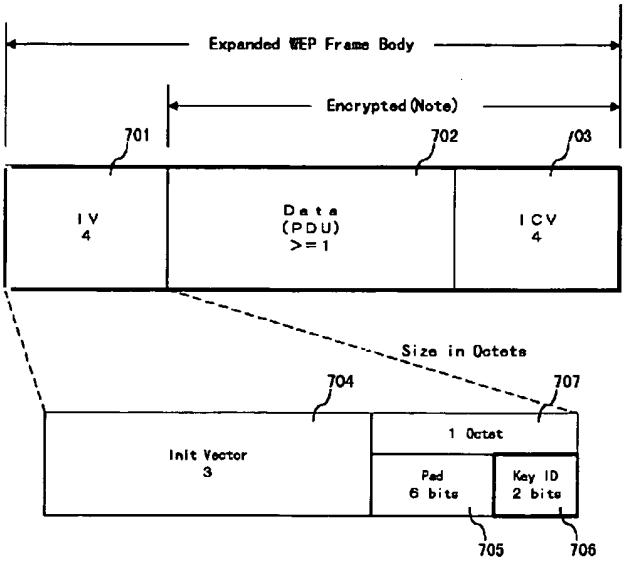
【図3】


301
制御手段
308
鍵ID生成手段
309
IV生成手段
302
暗号鍵設定手段
303
第1鍵記憶手段
307
304
第3鍵記憶手段
鍵選択手段
305
第3鍵記憶手段
306
第4鍵記憶手段
310
平文入力手段
316
鍵ID抽出手段
311
WEP暗号化手段
312
暗号文送出手段
315
平文出力手段
314
WEP復号化手段
313
暗号文入力手段

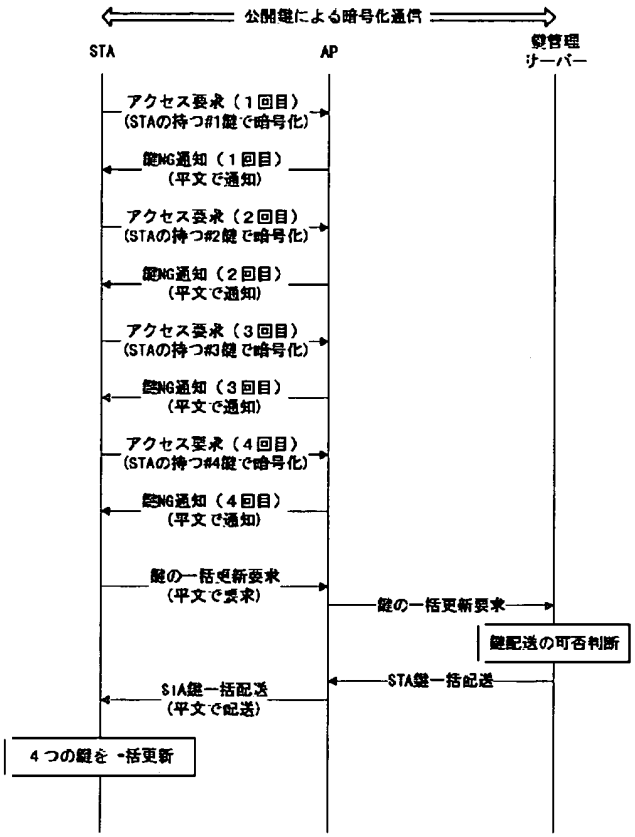
【図4】


STA
AP
鍵管理サーバー
n番の鍵更新
AP鍵配送
n番の鍵更新
鍵更新通知
(n番以外の鍵で暗号化)
鍵更新要求
(APが使用した鍵で暗号化)
鍵更新要求
鍵配送の可否判断
STA鍵配送
STA鍵配送
(n番以外の鍵で暗号化)
n番の鍵更新

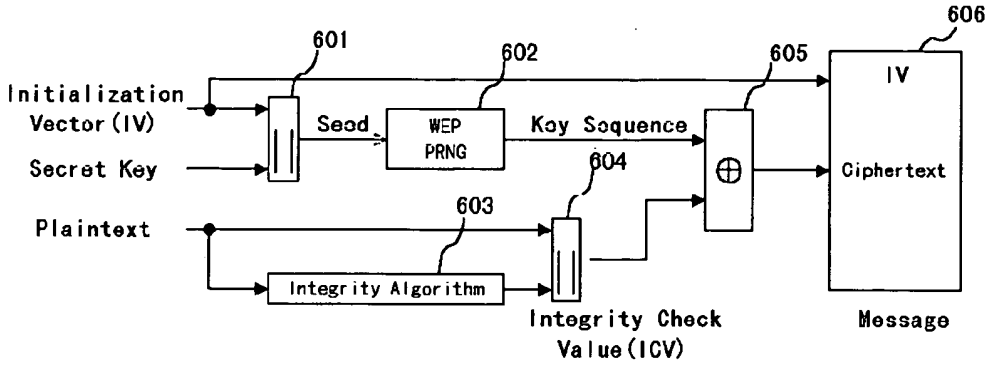
【図7】


Expanded WEP Frame Body
Encrypted (Note)
701
702
703
IV
4
Data
(PDU)
>=1
ICV
4
Size in Octets
704
707
Init Vector
3
1 Octet
Pad
6 bits
Key ID
2 bits
705
706

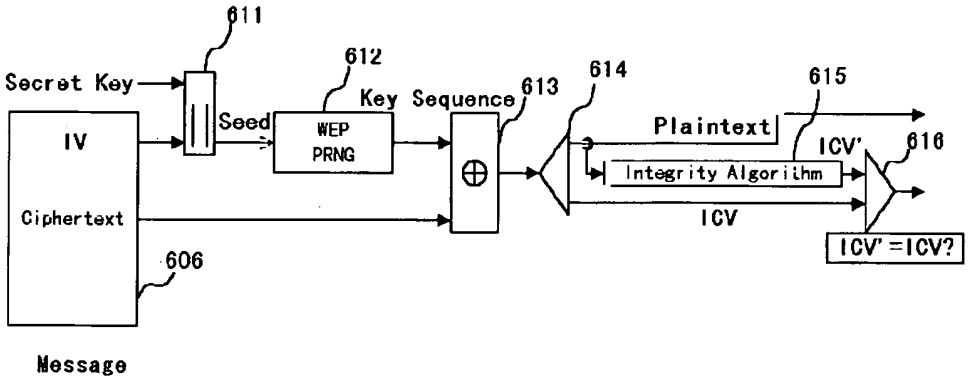
【図５】


公開鍵による暗号化通信
STA
AP
鍵管理サーバー
アクセス要求（１回目）
(STAの持つ#1鍵で暗号化)
鍵NG通知（１回目）
(平文で通知)
アクセス要求（２回目）
(STAの持つ#2鍵で暗号化)
鍵NG通知（２回目）
(平文で通知)
アクセス要求（３回目）
(STAの持つ#3鍵で暗号化)
鍵NG通知（３回目）
(平文で通知)
アクセス要求（４回目）
(STAの持つ#4鍵で暗号化)
鍵NG通知（４回目）
(平文で通知)
鍵の一括更新要求
(平文で要求)
鍵の一括更新要求
鍵配送の可否判断
STA鍵一括配送
STA鍵一括配送
(平文で配送)
４つの鍵を一括更新

【図6】


601
602
605
606
Initialization Vector (IV)
Secret Key
Seed
WEP PRNG
Key Sequence
IV
Ciphertext
604
603
Plaintext
Integrity Algorithm
Integrity Check Value (ICV)
Message

(a)


611
612
613
614
615
616
Secret Key
Seed
WEP PRNG
Key Sequence
Plaintext
ICV'
Integrity Algorithm
ICV
ICV'=ICV?
IV
Ciphertext
606
Message

(b)